Exhibit A

Order of Consolidation (12/01/24) CCCH 0622

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

STATE OF ILLINOIS
COUNTY OF COOK | SS:

8087
8202

Lynell Long, individually and on behalf of all others similarly situated,

v.

Medical Express Ambulance Service, Inc. d/b/a Medex Ambulance,

Case No. 25 CH 4521

ORDER OF CONSOLIDATION

This matter coming on to be heard on a Motion for Consolidation before Judge Sophia H. Hall, Interim Acting Presiding Judge of the Chancery Division.

◉ 4216 IT IS HEREBY ORDERED that the motion is granted and this cause be consolidated with case number #: 25 CH 4441

now pending on Chancery Calendar Number # 8 before Judge Michael T. Mullen.

○ 5216 IT IS HEREBY ORDERED that the motion is denied.

ENTERED
Judge Sophia H. Hall - 0162
MAY 28 2025
MARIYANA T. SPYROPOULOS
CLERK OF THE CIRCUIT COURT
OF COOK COUNTY, IL

Sophia H. Hall
Presiding Judge
Chancery Division

Judge No. 0162

5/28/25

Exhibit B

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

CHRISTOPHER DIXON, individually and on behalf all others similarly situated, Plaintiff, v. MEDICAL EXPRESS AMBULANCE SERVICE, INC. d/b/a MEDEX AMBULANCE, Defendant.	Case No. 2025CH04441 Consolidated with the below-captioned cases
LYNELL LONG, individually and on behalf all others similarly situated, Plaintiff, v. MEDICAL EXPRESS AMBULANCE SERVICE, INC., Defendant.	Case No. 2025CH04521
DANIEL ELLER, individually and on behalf all others similarly situated, Plaintiff, v. MEDICAL EXPRESS AMBULANCE SERVICE INC., d/b/a MEDEX AMBULANCE, Defendant.	Case No. 2025CH04528

MICHAEL GORSKI, individually and on behalf all others similarly situated, Plaintiff, v. MEDICAL EXPRESS AMBULANCE SERVICE, INC. d/b/a MEDEX AMBULANCE, Defendant.	Case No. 2025CH04560
ANDRE GLENN, individually and on behalf all others similarly situated, Plaintiff, v. MEDICAL EXPRESS AMBULANCE SERVICE, INC., d/b/a MEDEX AMBULANCE, Defendant.	Case No. 2025CH04621

ORDER

A hearing was held on June 13, 2025, regarding Plaintiffs' Motion to Appoint Interim Co-Lead Class Counsel. It is hereby ordered:

1. Plaintiffs' Motion to Appoint Interim Co-Lead Class Counsel is GRANTED. The Court appoints Ben Barnow of Barnow and Associates, P.C., Elena A. Belov of the Almeida Law Group LLC, Nickolas J. Hagman of Cafferty Clobes Meriwether & Sprengel LLP, and Cassandra Miller of Strauss Borrelli PLLC as Interim Co-Lead Class Counsel. Interim Co-Lead Class Counsel have the following responsibilities:

   a. Finalizing and filing all pleadings, briefs, motions, and other papers on behalf of Plaintiffs and the putative class;
   b. Initiating, coordinating, and conducting all pretrial discovery for the benefit of Plaintiffs and the putative class, including causing the issuance of interrogatories, document requests, requests for admission, subpoenas, and examining witnesses at depositions;
   c. Conducting all settlement negotiations on behalf of Plaintiffs and the putative class;
   d. Acting as the spokesperson for Plaintiffs and the putative class at pretrial proceedings in response to the Court's inquiries, subject to any right of

individual Plaintiffs' counsel to present non-repetitive, individual or different positions as directed by the Court;

e. Conducting trial and post-trial proceedings;
f. Conducting all appeals;
g. Consulting with and employing consultants and experts as they may deem appropriate;
h. Negotiating and entering into stipulations with Defendant regarding the litigation;
i. Monitoring the activities of plaintiffs' counsel to ensure that schedules are met and unnecessary expenditures of time and money are avoided;
j. Coordinating and communicating with Defendant's counsel with respect to the matters addressed in this paragraph; and
k. Performing such functions as may be expressly authorized by further orders of the Court.

2. Plaintiffs' deadline to file a consolidated complaint is July 28, 2025. Plaintiffs shall deliver hard copies of the consolidated complaint to chambers.

3. Defendant's responsive pleading deadline for all the above-captioned matters is stayed pending the forthcoming consolidated complaint.

4. A hearing regarding Defendant's responsive pleading with respect to the consolidated complaint is set for August 13, 2025, at 9:30am via Zoom (Zoom Meeting ID Number: 966 9558 1801; Password: 160424).

/s/ Michael T. Mullen
Hon. Michael T. Mullen

Order Prepared By:
Riley W. Prince (ARDC #6339536)
Barnow and Associates, P.C.
205 W. Randolph St., Ste. 1630
Chicago, IL 60606
rprince@barnowlaw.com

Judge Michael T. Mullen

JUN 13 2025

Circuit Court - 2084

Exhibit C

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

CHRISTOPHER DIXON, DANIEL ELLER, ANDRE GLENN, MICHAEL GORSKI, JONATHAN KAHANOVITCH, and LYNELL LONG, on behalf of themselves and all others similarly situated, Plaintiffs, v. MEDICAL EXPRESS AMBULANCE SERVICE, INC. d/b/a MEDEX AMBULANCE, Defendant.	Case No. 2025CH04441 Consolidated with Case Nos.: 2025CH04521 2025CH04528 2025CH04560 2025CH04621 CLASS ACTION DEMANDED JURY TRIAL

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Christopher Dixon, Daniel Eller, Andre Glenn, Michael Gorski, Jonathan Kahanovitch, and Lynnell Long ("Plaintiffs") bring this class action against Medical Express Ambulance Service, Inc. d/b/a MedEx Ambulance ("Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this consolidated class action lawsuit against Defendant for its failure to properly secure and safeguard Plaintiffs' and other similarly situated current and former patients' and employees' (collectively defined herein as the "Class" or "Class Members") personally identifiable information ("PII") and protected health information ("PHI" and collectively with PII, the "Private Information") from cybercriminals.

2. MedEx operates an ambulance service in the Chicago area, including provision of basic life support and advanced life support ambulance services to the general population.

3. As part of its business, Defendant collects a treasure-trove of data from its customers and employees, including highly sensitive Private Information.

4. On or about March 18, 2024, MedEx experienced a breach of its network security systems (the "Data Breach"). MedEx did not report the breach—which affected at least 118,418 individuals—until at least April 14, 2025, or ***over a year*** after the cyberattack took place.[1]

5. In the Data Breach, an unauthorized third party gained access to Private Information of Defendant's patients and employees including their: name, date of birth, demographic information, Social Security number, driver's license number, medical information, financial claims information, and health insurance information.

6. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect against disclosure—was targeted, compromised, and unlawfully accessed due to the Data Breach.

7. Healthcare providers that handle Private Information, like Defendant, have an obligation to employ reasonable and necessary data security practices to protect the sensitive, confidential and personal information entrusted to them.

8. This duty exists because it is foreseeable that the exposure of such Private Information to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, medical and financial identity theft, invasion of their private health matters and other long-term issues.

---

[1] *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e8fc85b0-09a9-4d0b-b6ee-b38d4ccfa768.html (last visited July 28, 2025)..

9. The harm resulting from a data and privacy breach manifests in several ways, including identity theft as well as financial and medical fraud, and the exposure of a person's Private Information through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives.

10. Mitigating that risk requires individuals to devote significant time, money and other resources to closely monitor their credit, financial accounts, health records and email accounts, as well as several additional prophylactic measures.

11. In this instance, all of that could have been avoided if Defendant had employed reasonable and appropriate data security measures.

12. On or about April 14, 2025, Defendant disclosed that it "recently experienced a data security incident that may have resulted in unauthorized access to patient health information and employee personal information."[2]

13. Defendant's "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach has been severely diminished.

14. As a direct and proximate result of Defendant's failure to implement and follow basic security procedures, Plaintiffs' and Class Members' PII and PHI is now in the hands of cybercriminals.

[2] *See Notice of Data Security Incident*, MEDEX AMBULANCE (April 14, 2025), https://medexambulance.com/home/notice-of-data-breach/.

15. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, dissemination of Private Information on the dark web, and similar forms of criminal mischief, risk which may last for the rest of their lives.

16. Plaintiffs and Class Members have also suffered concrete injuries in fact including, but not limited to, lost or diminished value of Private Information, lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, loss of benefit of the bargain, lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, and actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails.

17. Consequently, Plaintiffs and Class Members must devote substantially more time, money and energy to protect themselves, to the extent possible, from these crimes.

18. Plaintiffs, on behalf of themselves and all others similarly situated, therefore bring claims for (i) Negligence; (ii) Breach of Implied Contract; (iii) Breach of Fiduciary Duty; (iv) Invasion of Privacy; (v) Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, *et seq.* ("ICFA"); (vi) Unjust Enrichment; and (vii) Declaratory Judgment. Plaintiffs seek damages and injunctive relief, including the adoption of reasonably necessary and appropriate data security practices to safeguard the Private Information in Defendant's custody in order to prevent incidents like the Data Breach from occurring in the future.

PARTIES

Representative Plaintiffs

19. Plaintiff Christopher Dixon is a resident and citizen of Chicago, Illinois and is a former employee of Defendant.

20. Plaintiff Daniel Eller Dixon is a resident and citizen of Chicago, Illinois and is a former employee of Defendant.

21. Plaintiff Andre Glenn is a citizen of Dolton, Illinois and a former employee of Defendant.

22. Plaintiff Michael Gorski is a resident and citizen of Chicago, Illinois and is a former employee of Defendant.

23. Plaintiff Jonathan Kahanovitch is a resident and citizen of Chicago, Illinois and is a former employee of Defendant

24. Plaintiff Lynnell Long is a resident and citizen of Chicago, Illinois and is a former employee of Defendant.

25. Plaintiffs understandably and reasonably believed and trusted that their Private Information provided to Defendant in the course of their employment by MedEx would be kept confidential and secure and would be used only for authorized purposes.

Defendant Medical Express Ambulance Service, Inc.

26. Defendant Medical Express Ambulance Service, Inc., d/b/a MedEx Ambulance is an Illinois corporation with its principal place of business located at 5650 W. Howard Street, Skokie, IL 60077.

27. Defendant is a corporation that provides ambulance and other healthcare-related travel services to the Chicago metropolitan area.[3]

[3] *See Our Story & Mission*, MEDEX AMBULANCE, https://medexambulance.com/our-story/ (last visited July 28, 2025).

JURISDICTION AND VENUE

28. This Court has general personal jurisdiction over MedEx pursuant to 735 ILCS 5/2-209 because MedEx is organized under the laws of this State and regularly does business or solicits business, engages in other persistent courses of conduct, and derives substantial revenue from services provided to individuals in Cook County and in the State of Illinois, and expects or should reasonably expect to be in court here.

29. This Court has subject matter jurisdiction over this matter pursuant to Ill. Const. 1970, art. VI, § 9.

30. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101 because MedEx resides in this County, conducts its usual and customary business in this County, and because a substantial portion of the events complained of occurred in this County.

COMMON FACTUAL ALLEGATIONS

A. *MedEx Collects a Significant Amount of Private Information.*

31. MedEx is an ambulance service that was founded in 1998.[4] MedEx provides "services to hundreds of healthcare facilities throughout the Chicagoland area."[5] These facilities include "Lurie Children's Hospital, University of Chicago Medicine, University of Illinois Hospital, Kindred Hospitals of Chicago, and Swedish Covenant Hospital."[6]

32. In the regular course of its business, MedEx collects and maintains the Private Information of its current and former patients and employees. MedEx required Plaintiffs and Class

[4] *Id.*

[5] *Id.*

[6] *Id.*

members to provide it with their Private Information as a condition of providing them with healthcare services or employment.

33. MedEx's website contains a Privacy Policy (the "Privacy Policy"), which it provides to those from whom it collects Private Information, which describes how Plaintiffs' and Class members' Private Information may be used and disclosed by MedEx.[7]

34. MedEx tells those that it collects Private Information from that it "is required by law to maintain the privacy of certain confidential health care information, known as Protected Health Information or PHI . . . ."[8] It also states that it "respect[s] [their] privacy and treat[s] all healthcare information about [its] patients with care under strict policies of confidentiality that all of [its] staff are committed to following at all times."[9]

35. The Privacy Policy contains a list of instances in which it may share Private Information with others.[10] None of the instances include a cyberattack.

36. Plaintiffs and Class members are current or former patients or employees of MedEx who entrusted MedEx with their Private Information.

B. *The Data Breach*

37. On or about April 14, 2025, Defendant posted a notice to its website (the "Notice"), stating, among other things, that "[o]n March 18, 2024, MedEx experienced a network disruption that impacted the functionality and access of certain systems . . . . The forensic investigation determined that personal information may have been acquired by the threat actor." It also stated

---

[7] *Privacy Practices*, MEDEX AMBULANCE, https://medexambulance.com/wp-content/uploads/2023/05/Medex-Privacy-Practices.pdf [hereinafter, the "*Privacy Policy*"] (last visited July 28, 2025).

[8] *Id.*

[9] *Id.*

[10] *Id.*

that "the following information related to potentially impacted individuals may have been subject to unauthorized access: Name; date of birth; demographic information, Social Security number, driver's license number; state identification number; medical information; financial information; health insurance information; username and password; and for some, passport information."[11]

38. Omitted from the Notice were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

39. Although the Notice is lacking in details, it does provide the following: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's network and systems, the cybercriminals targeted information including Plaintiffs' and Class Members' Social Security numbers, PHI, and other sensitive information for download and theft.

40. Incredibly, Defendant has attempted to shift responsibility for lost Private Information to the victims of its Data Breach, stating: "We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a

[11] *See* MedEx's *Notice*, *supra* note 2.

breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file."[12]

41. Defendant had obligations created by the FTC Act, HIPAA, contract, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

42. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its patients' and employees' PII and PHI.

43. Furthermore, despite discovering the Data Breach on March 18, 2024, Defendant waited an entire year before notifying affected individuals and regulatory authorities, with notifications not occurring until March 2025.[13]

44. This unreasonable delay in reporting the breach significantly impeded Plaintiffs' and Class Members' ability to take timely protective measures to safeguard their Private Information and mitigate potential harm.

45. This delay also violated HIPAA's Breach Notification Rule, which requires covered entities to provide notification to affected individuals "without unreasonable delay and in no case later than 60 days following discovery of the breach." 45 C.F.R. §§ 164.400-414.

46. Defendant's failure to promptly notify victims of the Data Breach further demonstrates its negligent approach to data security and regulatory compliance.

[12] *Id.*
[13] *Id.*

C. *Defendant Knew the Risks of Storing Valuable Private Information and the Foreseeable Harm to Victims.*

47. Defendant was well aware that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

48. Defendant also knew that a breach of its systems—and exposure of the information stored therein—would result in the increased risk of identity theft and fraud (financial and medical) against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

49. These risks are not merely theoretical; in recent years, numerous high-profile data breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem as well as countless ones in the healthcare industry.

50. PII has considerable value and constitutes an enticing and well-known target to hackers, who can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[14]

51. PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.[15]

52. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities.

---

[14] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[15] *See* Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

53. Indeed, in 2023, HHS' Office of Civil Rights ("OCR"), reported a 239% increase in hacking-related data breaches between January 1, 2018, and September 30, 2023, and a 278% increase in ransomware attacks over the same period.[16] In 2019, hacking accounted for 49% of all reported breaches, and in 2023, 79.7% of data breaches were due to hacking incidents.[17]

54. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years; for instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[18]

55. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[19]

56. Additionally, healthcare providers "store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly – making the industry a growing target."[20]

57. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information, In a 2025 report, Kroll found that "the healthcare industry was the most breached" in

---

[16] Steve Adler, *Healthcare Data Breach Statistics*, THE HIPAA JOURNAL (May 26, 2025), https://www.hipaajournal.com/healthcare-data-breach-statistics/.

[17] *Id*.

[18] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited July 28, 2025).

[19] *The healthcare industry is at risk*, Swivel Secure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited July 28, 2025).

[20] *Id.*

2024.[21] The company found that 23% of the breaches that it handled responses for were from the healthcare industry, up from 18% in 2023.[22]

58. The healthcare sector suffered about 337 breaches in the first half of 2022 alone according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[23]

59. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients and employees especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

60. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "[m]edical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[24]

61. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.

---

[21] *Data Breach Outlook*, KROLL, https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2025 (last visited July 28, 2025).

[22] *See id*.

[23] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

[24] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[25]

62. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

63. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email

[25] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

64. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

65. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[26] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

66. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

67. For example, Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security

[26] *Did you get a data breach notice?*, FTC, https://www.identitytheft.gov/Steps (last visited July 28, 2025).

Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[27]

It is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

68. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

69. There may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused.

70. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before

---

[27] *Identity Theft and Your Social Security Number*, SSA https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 28, 2025).

[28] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back* (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[29]

71. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

72. Based on the value of its patients' and employees' PII and PHI to cybercriminals, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

D. *The Data Breach Was Preventable.*

73. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

[29] *Report to Congressional Requesters, Personal Information*, GAO (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited July 28, 2025).

74. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

75. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented numerous measures as recommended by the United States Government, including but not limited to:

- Implementing an awareness and training program.
- Enabling strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scanning all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configuring firewalls to block access to known malicious IP addresses.
- Setting anti-virus and anti-malware programs to conduct regular scans automatically.
- Managing the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.[30]

76. Given that Defendant was storing the Private Information of its current and former patients and employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

77. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of more than one hundred thousand individuals, including that of Plaintiffs and Class Members.

[30] How to Protect Your Networks from RANSOMWARE, at 3, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited July 28, 2025).

E. ***Defendant is Obligated Under HIPAA to Safeguard Private Information.***

78. Defendant is required by HIPAA to safeguard patient PHI.

79. Defendant is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

80. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

81. Further to 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

82. Under C.F.R. 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

83. HIPAA requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

84. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[31]

85. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiffs or Class Members consent to the disclosure of their PHI to cybercriminals.

86. As such, Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and Class Members' PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

87. Given the application of HIPAA to Defendant, and that Plaintiffs and Class Members entrusted their PHI to Defendant in order to receive healthcare services, Plaintiffs and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

F. *FTC Guidelines Prohibit Defendant from Engaging in Unfair or Deceptive Acts or Practices.*

88. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

[31] *Breach Notification Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited July 28, 2025).

89. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[32]

90. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[33]

91. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[34]

92. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[32] *Start with Security – A Guide for Business*, FTC (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 28, 2025).

[33] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 28, 2025).

[34] *Id.*

93. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

94. Defendant was at all times fully aware of its obligations to protect the PII and PHI of patients and employees because of its position as a healthcare provider and/or employer, which gave it direct access to reams of patient and staff PII and PHI. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. *Defendant Violated Industry Standards.*

95. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data.

96. Other best cybersecurity practices that are standard for healthcare entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

97. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

98. These foregoing frameworks are existing and applicable industry standards for healthcare entities, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

H. *The Monetary Value of Plaintiffs' and Class Members' Private Information.*

99. As a result of Defendant's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information.

100. From a 2013 study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identifying fraud is only about 3%.[35]

101. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[36]

102. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[37]

---

[35] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4 (Mar. 7, 2013), https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.

[36] *Id.*

[37] Andrew Steger, *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

103. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

104. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[38]

105. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

106. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[39]

---

[38] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[39] *See* U.S. Dep't of Justice, *Victims of Identity Theft* (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf.

107. The value of Plaintiffs' and Class Members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[40]

108. This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

109. Health information, in particular, is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[41]

110. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[42]

111. The Federal Trade Commission has warned consumers of the dangers of medical identity theft, stating that criminals can use personal information like a "health insurance account number or Medicare number" to "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." The FTC further warns that

[40] *Data Breaches: In the Healthcare Sector*, CIS, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited July 28, 2025).
[41] *Id.*
[42] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.

instances of medical identity theft "could affect the medical care you're able to get or the health insurance benefits you're able to use[,]" while also having a negative impact on credit scores.[43]

112. Here, where health insurance information was among the Private Information impacted in the Data Breach, Plaintiffs' and Class Members' risk of suffering future medical identity theft is especially substantial.

113. The ramifications of Defendant's failure to keep its patients' and employees' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for 6 to 12 months or even longer.

114. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[44] This gives thieves ample time to seek multiple treatments under the victim's name.

115. Indeed, when compromised, healthcare-related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[45]

116. Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent

[43] *What to Know About Medical Identity Theft*, FTC, https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited July 28, 2025).
[44] *See Medical ID Theft Checklist*, IDENTITY FORCE, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited July 28, 2025).
[45] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft, including medical identity theft, have a crippling effect on individuals and detrimentally impact the economy as a whole.[46]

117. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft (including medical identity theft) and fraud.

118. Upon information and good faith belief, had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented the ransomware attack into their systems and, ultimately, the theft of the Private Information of patients and employees within their systems.

119. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves.

120. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[47] For example,

[46] *Id.*

[47] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, at 35-38, FTC (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[48]

121. Based upon information and belief, the unauthorized parties have already utilized, and will continue utilize, the Private Information they obtained through the Data Breach to obtain additional information from Plaintiffs and Class Members that can be misused.

122. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

123. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

124. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

125. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

126. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

[48] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

I. *Plaintiffs and Class Members Have Suffered Compensable Damages.*

127. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways.

128. The risks associated with identity theft, including medical identity theft, are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

129. In order to mitigate against the risks of identity theft and fraud, Plaintiffs and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

130. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

131. Further, the value of Plaintiffs' and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

132. Plaintiffs and Class Members now face a greater risk of identity theft, including medical and financial identity theft.

133. Plaintiffs and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' and employees' PII and PHI.

134. Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

135. Plaintiffs and Class Members also did not receive the full benefit of their bargain when paying for medical services. Instead, they received services of a diminished value to those described in their agreements with Defendant. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

136. Plaintiffs and Class Members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

137. Finally, in addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

Plaintiff Christopher Dixon's Experience

138. Plaintiff Christopher Dixon was an employee of Defendant who worked for Defendant around 2016.

139. As a condition of employment with Defendant, he was required to provide his Private Information to Defendant, including his Social Security number and health insurance information.

140. Upon information and good faith belief, Defendant maintained Plaintiff Dixon's Private Information in its systems at the time of the Data Breach.

141. Plaintiff Dixon is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. He would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

142. Upon information and belief, Plaintiff Dixon's Private Information was compromised in the Data Breach.

143. Plaintiff Dixon made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, and monitoring his financial accounts for any unusual activity, which may take years to detect. He has spent significant time dealing with the Data Breach -- valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

144. Plaintiff Dixon suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

145. Plaintiff Dixon additionally suffered actual injury in the form of his Private Information being disseminated on the dark web -- on information and belief, as a result of the Data Breach – as evidenced by dark web alerts he has received regarding his passwords.

146. The Data Breach has caused Plaintiff Dixon to suffer fear, anxiety, and stress, which has been compounded by an increase in spam communications and by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

147. As a result of the Data Breach, Plaintiff Dixon anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

148. As a result of the Data Breach, Plaintiff Dixon is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

149. Plaintiff Dixon has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Daniel Eller's Experience

150. Plaintiff Daniel Eller is a former employee of Defendant and a victim of the Data Breach.

151. As a condition of receiving employment, Defendant required Plaintiff Eller to provide his Private Information, including at least his name and Social Security Number.

152. Plaintiff Eller received Defendant's Notice despite having not worked for Defendant for approximately 9 years. Plaintiff Eller reasonably believed that Defendant exercised industry-standard data retention requirements, and that any of his Private Information that Defendant had once stored in its systems would have long since been destroyed.

153. Plaintiff Eller provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and for unknown reasons continues to maintain Plaintiffs' Private Information and therefore has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure, or to destroy it.

154. Upon information and belief, through its Data Breach, Defendant compromised Plaintiff Eller's PII, including at least his name and Social Security number. And upon information and belief, Plaintiff Eller's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

155. To the best of his knowledge, Plaintiff Eller's PII has not been compromised in any prior data breaches.

156. Plaintiff Eller fears for his personal financial security and worries about what information was exposed in the Data Breach.

157. Because of the Data Breach, Plaintiff Eller has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Eller's injuries are precisely the type of injuries that the law contemplates and addresses.

158. Plaintiff Eller suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

159. Plaintiff Eller suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

160. Plaintiff Eller suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Eller's Private Information right in the hands of criminals.

161. Plaintiff Eller began experiencing a substantial increase in spam and scam text messages and phone calls, that his PII has been placed in the hands of cybercriminals.

162. On information and belief, Plaintiff Eller's phone number was also compromised as a result of the Data Breach, as cybercriminals are able to use an individual's PII that is accessible on the dark web, to gather and steal even more information.

163. Because of the Data Breach, and in accordance with Defendant's instructions in its Notice, Plaintiff Eller spent time taking steps to mitigate the impact of the Data Breach.

164. Today, Plaintiff Eller has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains in Defendant's possession—is protected and safeguarded from additional breaches.

165. As a condition of receiving employment, Defendant required Plaintiff Eller to provide his Private Information, including at least his name and Social Security number.

166. Plaintiff Eller was shocked when he received Defendant's Notice on or around April 20, 2025, because he has not worked for Defendant for approximately 9 years. He reasonably believed that Defendant exercised industry-standard data retention requirements, and that any of his Private Information would have long since been destroyed.

167. Upon information and belief, Plaintiff Eller's name and Social Security number were compromised in the Data Breach.

168. Following the Data Breach, Plaintiff Eller began experiencing a substantial increase in spam text messages and phone calls and has spent time researching credit monitoring services to mitigate any harm.

Plaintiff Michael Gorski's Experience

169. Plaintiff Michael Gorski was an employee of Defendant who worked for Defendant from approximately 2015-2017.

170. As a condition of employment with Defendant, he was required to provide his Private Information to Defendant, including his Social Security number and health insurance information.

171. Upon information and good faith belief, Defendant maintained Plaintiff Gorski's Private Information in its systems at the time of the Data Breach.

172. Plaintiff Gorski received Defendant's Notice despite having not worked for Defendant for several years. Plaintiff Gorski reasonably believed that Defendant exercised industry-standard data retention requirements, and that any of his Private Information that Defendant had once stored in its systems would have long since been destroyed.

173. Plaintiff Gorski is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

174. Upon information and belief, Plaintiff Gorski's Private Information was compromised in the Data Breach.

175. Plaintiff Gorski made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, and monitoring his financial accounts for any unusual activity, which may take years to detect. Plaintiff Gorski has spent significant time dealing with the Data Breach -- valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

176. Plaintiff Gorski suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii)

nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

177. Plaintiff Gorski additionally suffered actual injury in the form of his Private Information being disseminated, on information and belief, on the dark web as a result of the Data Breach, as evidenced by dark web alerts he has received regarding his passwords.

178. The Data Breach has caused Plaintiff Gorski to suffer fear, anxiety, and stress, which has been compounded by an increase in spam communications and by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

179. As a result of the Data Breach, Plaintiff Gorski anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

180. As a result of the Data Breach, Plaintiff Gorski is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

181. Plaintiff Gorski has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Andre Glenn's Experience

182. Plaintiff Andre Glenn is a former employee of Defendant.

183. As a condition of providing employment to Plaintiff Glenn, Defendant required him to provide it with his Private Information.

184. Plaintiff Glenn believed MedEx had implemented and maintained reasonable security and practices to protect his PII/PHI. With this belief in mind, Plaintiff Glenn provided his PII/PHI to MedEx in connection with obtaining employment from MedEx. Had Plaintiff Glenn known that MedEx does not adequately protect the PII/PHI in its possession, he would not have obtained employment from MedEx or agreed to entrust it with his PII/PHI.

185. Plaintiff Glenn received notice from Defendant notifying him that his Private Information was affected in the Data Breach.

186. After the Data Breach occurred, Plaintiff Glenn has experienced an increase in the number of spam text messages and emails that he receives.

187. Since learning of the Data Breach, Plaintiff Glenn has spent time researching credit monitoring services to mitigate any harm.

188. Plaintiff Glenn suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

189. As a result of the Data Breach, Plaintiff Glenn anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, he is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Jonathan Kahanovitch's Experience

190. Plaintiff Jonathan Kahanovitch is a former employee of Defendant and a victim of the Data Breach, having worked for Defendant from on or around 2018 to on or around 2019.

191. As a condition of receiving employment, Defendant required Plaintiff Kahanovitch to provide his Private Information, including at least his name and Social Security Number.

192. Plaintiff Kahanovitch received Defendant's Notice despite having not worked for Defendant for approximately 6 years. Plaintiff Kahanovitch reasonably believed that Defendant exercised industry-standard data retention requirements, and that any of his Private Information that Defendant had once stored in its systems would have long since been destroyed.

193. Plaintiff Kahanovitch provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and for unknown reasons continues to maintain Plaintiff Kahanovitch's Private Information and therefore has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure, or to destroy it.

194. Plaintiff Kahanovitch is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. He would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

195. Upon information and belief, Plaintiff Kahanovitch's Private Information was compromised in the Data Breach.

196. Upon information and belief, through its Data Breach, Defendant compromised Plaintiff Kahanovitch's PII, including at least his name and Social Security number. And upon information and belief, Plaintiff Kahanovitch's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

197. Plaintiff Kahanovitch fears for his personal financial security and worries about what information was exposed in the Data Breach.

198. To the best of his knowledge, Plaintiff Kahanovitch's PII has not been compromised in any prior data breaches.

199. After the Data Breach on or around January 2025 and February 2025, Plaintiff Kahanovitch experienced fraudulent charges made to his SoFi and BMO Harris credit card accounts. As a result of the fraud, Plaintiff Kahanovitch was forced to spend time disputing the charges and replacing the compromised cards.

200. Plaintiff Kahanovitch made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, and monitoring his financial accounts for any unusual activity, which may take years to detect. He has spent significant time dealing with the Data Breach -- valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

201. Because of the Data Breach, Plaintiff Kahanovitch has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Kahanovitch's injuries are precisely the type of injuries that the law contemplates and addresses.

202. Plaintiff Kahanovitch suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

203. Plaintiff Kahanovitch suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

204. Plaintiff Kahanovitch suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Kahanovitch's Private Information right in the hands of criminals.

205. Because of the Data Breach, and in accordance with Defendant's instructions in its Notice, Plaintiff Kahanovitch spent time taking steps to mitigate the impact of the Data Breach.

206. Today, Plaintiff Kahanovitch has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Lynnell Long's Experience

207. Plaintiff Lynnell Long was employed by MedEx between 2008 and 2016.

208. Plaintiff Long received MedEx's data breach notice. The notice informed Plaintiff Long that her Private Information was improperly accessed and obtained by third parties.

209. As a result of the Data Breach, Plaintiff Long has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Long has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

210. As a result of the Data Breach, Plaintiff Long has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff Long is

concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

211. Plaintiff Long suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

212. As a result of the Data Breach, Plaintiff Long anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

213. Plaintiffs bring this class action on behalf of themselves and all other individuals who are similarly situated pursuant to 735 ILCS 5/2-801 *et seq*.

214. Plaintiffs seek to represent a Nationwide Class of persons to be defined as follows:

> All individuals residing in the United States whose PII and/or PHI was compromised in the Data Breach which occurred on Defendant's servers or about March 18, 2024, including all individuals in the United States who were sent a notice of the Data Breach (the "Nationwide Class").

215. Plaintiffs seek to represent an Illinois Subclass of persons to be defined as follows:

> All individuals residing in the State of Illinois whose PII and/or PHI was compromised in the Data Breach which occurred on Defendant's servers or about March 18, 2024, including all individuals in Illinois who were sent a notice of the Data Breach (the "Illinois Subclass").

216. The Nationwide Class and the Illinois Subclass are referred to herein as the Class.

217. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families, all judges assigned to hear any aspect of this litigation, their immediate family members, and those individuals who make a timely and effective election to be excluded from this matter using the correct protocol for opting out.

218. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

219. **Numerosity: (735 ILCS 5/2-801(1)):** Defendant reported to the Office of the Maine Attorney General that approximately 118,418 persons were affected by the Data Breach.[49] Accordingly, the members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable.

220. **Commonality: (735 ILCS 5/2-801(2)):** This action involved questions of law and fact common to the Class that predominate over any questions affecting solely individual members of the Class. Such common questions include but are not limited to:

a. Whether Defendant failed to timely notify Plaintiffs and Class Members of the Data Breach;

b. Whether Defendant had a duty to protect the PII and PHI of Plaintiffs and Class Members;

[49] *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e8fc85b0-09a9-4d0b-b6ee-b38d4ccfa768.html (last visited July 28, 2025).

c. Whether Defendant had respective duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Defendant had respective duties not to disclose the PII and PHI of Plaintiffs and Class Members for non-business purposes;

e. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiffs and Class Members;

f. Whether and when Defendant actually learned of the Data Breach;

g. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' PII and PHI, and breached its duties thereby;

h. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

i. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

j. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

k. Whether Defendant adequately addressed and fixed the vulnerabilities that allowed the Data Breach to occur;

l. Whether Defendant was negligent and that negligence resulted in the Data Breach;

m. Whether Defendant entered into an implied contract with Plaintiffs and Class Members;

n. Whether Defendant breached that contract by failing to adequately safeguard Plaintiffs' and Class Members' PII and PHI;

o. Whether Defendant was unjustly enriched;

p. Whether Plaintiffs and Class Members are entitled to actual, statutory, and/or nominal damages as a result of Defendant's wrongful conduct; and

q. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

221. **Typicality: (735 ILCS 5/2-801(3)):** Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the

same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class were all patients or employees, or family members or caregivers of patients, of Defendant, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

222. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenges of these policies hinge on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

223. **Adequacy of Representation: (735 ILCS 5/2-801(4)):** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the members of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and have no interests antagonistic to the members of the Class. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above.

224. **Superiority and Manageability:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision

by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

225. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

226. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

227. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

228. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

229. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

230. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

231. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant breached its duty to Plaintiffs and Class Members, then Plaintiffs and each Class member suffered damages by that conduct.

232. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under 735 ILCS 5/2-801(4) and Illinois case law regarding class-wide injunctive relief.

233. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(*On behalf of Plaintiffs & the Nationwide Class*)

234. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

235. Plaintiffs bring this claim individually and on behalf of the Class.

236. Defendant owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

237. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

238. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

239. Defendant's duty also arose from Defendant's position as healthcare provider. Defendant holds itself out as trusted providers of healthcare, and thereby assumes a duty to reasonably protect its patients' and employees' information. Indeed, Defendant was in a unique

and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

240. Defendant breached the duties owed to Plaintiffs and Class Members and thus were negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiffs' and Class Members' Private Information, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to their patients and employees; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive Private Information.

241. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

242. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. The diminished value of the services they paid for and received, and

k. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

243. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(*On behalf of Plaintiffs & the Nationwide Class*)

244. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

245. Plaintiffs bring this claim individually and on behalf of the Class.

246. When Plaintiffs and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiffs' and Class Members' Private Information, comply with their statutory and common law duties to protect Plaintiffs' and Class Members' Private Information, and to timely notify them in the event of a data breach.

247. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's provision of healthcare services. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

248. Implicit in the agreement between Plaintiffs and Class Members and Defendant, was Defendant's obligation to: (a) use such Private Information for business purposes only; (b) take reasonable steps to safeguard Plaintiffs' and Class Members' Private Information; (c) prevent unauthorized access and/or disclosure of Plaintiffs' and Class Members' Private Information; (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their Private Information; (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized access and/or disclosure; and (f) retain Plaintiffs' and Class Members' Private Information under conditions that kept such information secure and confidential.

249. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with their statutory and common law duties to adequately protect Plaintiffs' and Class Members' Private Information and to timely notify them in the event of a data breach.

250. Plaintiffs and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their Private Information from unauthorized access and disclosure. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

251. Plaintiffs and Class Members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

252. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

253. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard their Private Information and by failing to provide them with timely and accurate notice of the Data Breach

254. The losses and damages Plaintiffs and Class Members sustained, include, but are not limited to:

a. Theft of their Private Information;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

255. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

256. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strength its data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) immediately provide and continue to provide adequate credit monitoring to Plaintiffs and all Class Members.

COUNT III
BREACH OF FIDUCIARY DUTY
(*On behalf of Plaintiffs & the Nationwide Class*)

257. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

258. Given the relationship between Defendant and Plaintiffs and Class Members, where Defendant became guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

259. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their Private Information.

260. Because of the highly sensitive nature of the Private Information, Plaintiffs and Class Members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

261. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' Private Information.

262. Defendant also breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

263. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT IV
INVASION OF PRIVACY
(On behalf of Plaintiffs & the Nationwide Class)

264. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

265. Plaintiffs and the class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

266. Defendant owed a duty to its current and former patients and employees, including Plaintiffs and the class to keep this information confidential.

267. The unauthorized acquisition (*i.e.*, theft) by a third party of Plaintiffs' and Class Members' Private Information is highly offensive to a reasonable person.

268. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

269. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

270. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

271. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

272. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

273. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiffs and the class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the class to suffer damages (as detailed *supra*).

274. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

275. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the class since their Private Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

276. Plaintiffs and the class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and the Class.

277. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which

includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT V
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/2, *ET SEQ.* ("ICFA")
(*On behalf of Plaintiffs & the Illinois Subclass*)

278. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

279. Plaintiffs bring this claim individually and on behalf of the Illinois Subclass.

280. Defendant offered and continues to offer healthcare and other related services in the State of Illinois.

281. Plaintiffs and Class Members purchased and received healthcare or other services from Defendant for personal, family, or household purposes.

282. Defendant engaged in unlawful and unfair practices in violation of the ICFA by failing to, or contracting with companies that failed to, implement and maintain reasonable security measures to protect and secure Plaintiffs' and Illinois Subclass members' Private Information in a manner that complied with applicable laws, regulations, and industry standards.

283. Defendant makes explicit statements to their patients and employees that their Private Information will remain private.

284. Defendant's duties also arise from the Illinois Personal Information Protection Act, 815 ILCS 530/45(a) which requires:

> A data collector that owns or licenses or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS 530/45. Defendant violated this duty by failing to, or contracting with companies that failed to, implement reasonably secure data security policies.

285. Defendant further violated the ICFA by failing to notify their current and former patients and employees of the data breach in a timely manner. The Illinois Personal Information Protection Act requires entities that experience a data breach to notify Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10. Violation of the Illinois Personal Information Protection Act constitutes an unlawful practice under the ICFA. 815 ILCS 530/20.

286. Due to the Data Breach, Plaintiffs and Class Members have lost property in the form of their Private Information. Further, Defendant's failure to adopt, or contracting with companies that failed to adopt, reasonable practices in protecting and safeguarding their patients' and employees' Private Information will force Plaintiffs and Class Members to spend time or money to protect against identity theft. Plaintiffs and Class Members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendant's practice of collecting and storing Private Information without appropriate and reasonable safeguards to protect such information.

287. As a result of Defendant's violations of the ICFA, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Defendant's possession; (vi) future costs in

terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT VI
UNJUST ENRICHMENT
(*On behalf of Plaintiffs & the Nationwide Class*)

288. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein, and pleads the following count in the alternative.

289. Plaintiffs bring this claim individually and on behalf of the Class.

290. Upon information and belief, Defendant funded its data security measures from its general revenue including payments made by or on behalf of Plaintiffs and Class Members.

291. As such, a portion of the payments made by or on behalf of Plaintiffs and the class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

292. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased healthcare services from Defendant and/or their agents and in so doing provided Defendant with their Private Information.

293. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

294. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

295. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of data security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits and the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective data security measures.

296. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

297. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members conferred upon Defendant.

298. Defendant acquired Plaintiffs' and Class Members' Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

299. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

300. Plaintiffs and Class Members have no adequate remedy at law.

301. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

302. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

303. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them.

In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT VII
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(*On behalf of Plaintiffs & the Nationwide Class*)

304. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

305. Plaintiffs bring this claim individually and on behalf of the Class.

306. Under the 735 ILCS 5/2-701, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

307. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs' and Class Members' from further data breaches that compromise their Private Information. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and remains at imminent risk that further compromises of their Private Information will occur in the future.

308. Pursuant to its authority under 735 ILCS 5/2-701, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure patients' and employees' Private Information and to timely notify patients and employees of a data breach under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure patients' and employees' Private Information.

309. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' and employees' Private Information.

310. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant's properties.

311. The risk of another such breach is real, immediate and substantial.

312. If another breach of Defendant's store of patient data occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

313. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

314. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Christopher Dixon, Daniel Eller, Andre Glenn, Michael Gorski, Jonathan Kahanovitch, and Lynnell Long, on behalf of themselves and other Class Members, pray for judgment against Defendant Medical Express Ambulance Service, Inc. d/b/a MedEx Ambulance as follows:

A. an Order certifying the Nationwide Class and the Illinois Subclass, and appointing Plaintiffs and their Counsel to represent the Class;

B. equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;

E. an award of attorney fees, costs, and litigation expenses, as allowed by law;

F. prejudgment interest on all amounts awarded and

G. all such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs on behalf of themselves and other members of the proposed Class, hereby demands a jury trial on all issues so triable.

Dated: July 28, 2025

Respectfully submitted,

/s/ Ben Barnow

Ben Barnow (IL Bar No. 0118265)
Anthony L. Parkhill (IL Bar No. 6317680)
Riley W. Prince (IL Bar No. 6339536)
Nicholas W. Blue (IL Bar No. 6343317)
BARNOW AND ASSOCIATES, P.C.
Cook County Attorney No. 38957
205 West Randolph Street, Suite 1630

Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com
nblue@barnowlaw.com

David S. Almeida (IL Bar No. 6285557)
Elena A. Belov (ARDC 6345116)
ALMEIDA LAW GROUP LLC
Firm ID 100530
849 W. Webster Avenue
Chicago, Illinois 60614
T: (708) 529-5418
david@almeidalawgroup.com
elena@almeidalawgroup.com

Cassandra Miller
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
cmiller@straussborrelli.com

Daniel O. Herrera
Nickolas J. Hagman
Krishna K. Motta
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
kmotta@caffertyclobes.com

Brandon M. Wise (ARDC 6319580)
PEIFFER WOLF CARR KANE CONWAY & WISE, LLP
Firm ID: 62258
One US Bank Plaza, Suite 1950
St. Louis, Missouri 63101

Ph: 314.833.4825
bwise@peifferwolf.com

Attorneys for Plaintiffs and the Class

Exhibit D

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

Celia Cuevas,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 1:25-cv-4735
	)	
Medical Express Ambulance Services, Inc., d/b/a MedEx Ambulance	)	
	)	
Defendant.	)	

DECLARATION IN SUPPORT OF MOTION TO DISMISS

I, Lauren Rubinson, declare that the following statements are true and correct to the best of my knowledge:

1. I am over eighteen (18) years of age.

2. I am the founder of Medical Express Ambulance Services, Inc. ("MedEx") and I have been employed with MedEx since 1997. I currently hold the position of President and Chief Executive Officer. As a result of my employment with MedEx, I have personal knowledge of MedEx's business and operations and the facts contained in this declaration.

3. On April 14, 2025, MedEx – through a third-party vendor – mailed notification letters regarding a data security incident to 68,817 individuals in the United States, which were the U.S. individuals for whom MedEx had mailing address information. The third-party vendor conducted a search of the U.S. Postal Service's National Change of Address database shortly prior to mailing the letters to locate the most recent mailing address for those individuals.

4. For the 68,817 letters, the following chart details the number of letters that were mailed to each jurisdiction, in order from largest number of letters mailed to smallest.

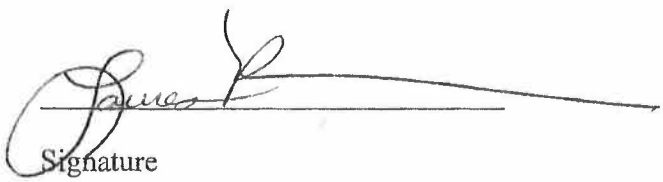
State	Number
IL	43,821
MI	2,322
IN	2,151
WI	1,700
CA	1,597
OH	1,323
TX	1,319
FL	1,264

MO	1,264
GA	1,062
NY	1,007
MN	949
CO	851
MA	714
IA	637
TN	636
NC	613
KY	473
VA	455
PA	446
KS	435
NJ	328
AZ	322
MD	319
AL	286
NE	249
WA	239
OK	182
SC	173
DC	168
AR	163
CT	157
PR	127
LA	124
NH	104
MS	103
NV	97
OR	97
NM	95
AK	49
ME	49
UT	48
RI	45
ND	39
VT	36
SD	32
MT	31
ID	29
DE	27

WY	22
HI	19
WV	18
VI	1
Total	**68,817**

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on August 2, 2025.

Lauren Rubinson



Signature